To: Committee on House Administration
Congressman Robert W. Ney (Ohio), Chairman
From: Professor Ronald L. Rivest
Viterbi Professor of Computer Science
Massachusetts Institute of Technology
Date: May 24, 2001
Re: Security in Voting Technology

Dear Chairman Ney and members of the Committee on House Administration:

I thank you for this opportunity to testify to your committee on issues of security in voting technology.

(I apologize for the brevity of these remarks, but I returned home from conferences in Europe only Monday night to discover your invitation for my testimony.)

I have been involved in the mathematical aspects of security for the last twenty-five years. I lead the Cryptography and Information Security group within MIT's Laboratory for Computer Science. I am a founder of RSA Data Security, a leading provider of security technology. Codes I have developed are used daily to secure millions of on-line Internet transactions.

For the past five years I have investigated the security of electronic voting. My students have implemented an electronic voting system used for student elections at MIT. I am currently participating in the CalTech/MIT Voting Technology Project; our initial report will be out this summer. The opinions expressed here are my own.

I find voting intriguing: it is not only important for our democratic society, but it is also technically challenging.

The challenge arises primarily from the need to remove voter's identities from their cast ballots, in order to prevent vote-buying and the coercion of voters. This requirement for anonymity makes electronic voting different than electronic commerce, where well-labeled receipts and well-labeled audit trails are standard. This requirement for anonymity can also make fraud easier, as the addition, deletion, or modification of anonymous ballots is harder to detect.

In 1869, inspired by the potential benefits of electricity, Thomas Alva Edison was granted U.S. patent 90,646 for an "Electric Vote-Recorder". Congress declined to use it, since it reported votes "too quickly" (!). Today, inspired by the potential benefits of computing and Internet technology, inventors and election system vendors are offering new voting technologies. We need to carefully assess what these new technologies can offer to see if they can really meet our needs.

Given the short time available, I would like to offer some personal opinions on the security of existing and prospective voting systems; I would be happy to expand further on any of these points in response to your questions.

(1) We are not ready for Internet voting from home.

-- I believe that voting equipment should be under the control of election officials. At least a decade of further research and development on the security of home computers is required before Internet voting from home should be contemplated.

(2) I believe that we should use the Internet to post:
(a) lists of registered voters
(b) list of actual voters
(c) list of actual ballots cast (not matched with voter's names, of course)

(3) As far as getting the biggest "bang for the buck" as far as security goes, I believe that we should
(a) improve voter registration procedures and the computerization of voter registration lists
(b) eliminate absentee balloting except for need.
I'm against voting by mail for convenience. I'd prefer having a national voting holiday and allowing voters to vote several weeks early at their town hall. Voters who vote absentee are simply not guaranteed the same freedom from coercion and bribery that ordinary voters have.

(4) I believe voting systems should have a physical audit trail. That audit trail should be directly created by the voter, or at least directly verifiable by the voter when he casts his vote. It need not be paper, but should be immutable and archival.

-- Many proposed electronic voting systems fail this requirement. Electronic voting systems offer improved ease-of-use and flexibility. They do not intrinsically offer improved security. (On the other hand, a physical audit trail is not a security panacea, although it is a big help.)

(5) We must ensure the highest degree of confidence that our elections are free of manipulation and fraud. The certification of voting systems should be an important part of this process.

However, it is difficult to certify complex software-based systems involving elaborate user interfaces and cryptographic functionality. Experts in computer security and cryptography need to be involved in the certification process. Requiring that all security-critical portions of the source code be "open-source" can greatly help to establish confidence in such complex systems.

But we are no more guaranteed protection against election fraud by buying flashy electronic equipment than we are guaranteed protection against fire by buying a shiny new fire engine. Security depends on the entire system, not just the components. We also need sound operational procedures managed by trained personnel. These operational procedures, which themselves should be documented and certified, should primarily ensure that no single person or vendor is ever in a position to compromise the integrity of our democratic process.

Finally, I note that we are in the midst of a technological revolution that provides both an enduring and improving set of opportunities and an increasing set of vulnerabilities. If there is a chance to improve things now, then our focus should not be on immediately spending money for new equipment, but rather on improving the higher-order processes of voting system research, evolution, certification, selection, financing, staffing, and oversight, as well as on improving voter education.

I thank you for your attention.